CLAIM LISTING

This listing of claims will replace all prior versions, and listings of claims in the application:

Amendments to the Claims

1. (Previously presented) In a programmable logic device (PLD) having a JTAG port, a decryptor for decrypting an encrypted bitstream, and a memory for storing decryption keys used by the decryptor to decrypt the encrypted bitstream, a method for loading the keys comprising:

placing the PLD into a printed circuit board;

testing the printed circuit board using the JTAG port of the PLD; and

loading the decryption keys into the memory using the JTAG port.

2. (Original) The method of Claim 1 wherein the step of loading the decryption keys into the memory is performed without also loading a design into the PLD.

3. (Original) The method of Claim 1 wherein the step of loading the decryption keys into the memory is performed without the use of a device programmer.

4. (Previously presented) A programmable logic device (PLD) comprising:

a test access port for testing the PLD; and

a circuit for loading at least one decryption key through the test access port.

5. (Original) The PLD of Claim 4 wherein the test access port is a JTAG port.

6. (Previously presented) The method of Claim 1, further comprising:

configuring the PLD for a non-secure mode prior to the loading the decryption keys; and

configuring the PLD for a secure mode after the loading the decryption keys.

7. (Previously presented) The method of Claim 6, further comprising:

erasing the decryption keys from the memory when configuring the PLD for the non-secure mode.

8. (Previously presented) The method of Claim 7, further comprising:

clearing a design from a configuration memory of the PLD when configuring the PLD for the non-secure mode.

9. (Previously presented) The method of Claim 1, further comprising:

reading the decryption keys using the JTAG port for verification.

10. (Previously presented) The PLD of Claim 4, further comprising:

a decryptor for decrypting an encrypted bitstream using the at least one decryption key.

11. (Previously presented) The PLD of Claim 10, further comprising:

a key memory for storing the at least one decryption key.

12. (Previously presented) The PLD of Claim 11, further comprising:

programmable logic;

configuration memory coupled to the programmable logic for configuring the programmable logic to perform a desired function; and

configuration logic coupled between the decryptor and the configuration memory for providing programming information to the configuration memory;

wherein the programming information comprises at least a portion of a decrypted bitstream provided by the decryptor.

13. (New) A programmable logic device (PLD), comprising:

a programmable logic arrangement and configuration memory coupled to the programmable logic arrangement;

a configuration control circuit coupled to the configuration memory and to a configuration port, the configuration control circuit adapted to store configuration data in the configuration memory;

a boundary scan control circuit coupled to a scan port and to the configuration control circuit;

a key memory coupled to the boundary scan control circuit, the key memory adapted to store at least one decryption key input via the scan port, transition to one of a secure mode and an non-secure mode in response to a control signal from the boundary scan control circuit, disable read and write of the key memory via the boundary scan control circuit in response to the key memory operating in the secure mode, and enable read and write of the key memory via the boundary scan control circuit in response to the key memory operating in the non-secure mode; and

a decryptor coupled to the configuration control circuit and to the key memory, the decryptor adapted to read the at least one decryption key from the key memory and decrypt an encrypted configuration bitstream from the configuration control circuit.

14. (New) The PLD of claim 13, wherein the key memory is further adapted to erase each decryption key from the key memory in response to transition of the key memory from the secure mode to the non-secure mode.

15. (New) The PLD of claim 14, wherein:

the key memory is further adapted to output to the configuration control circuit a security mode signal that indicates a current operating mode of the key memory; and

the configuration control circuit is further adapted to clear the configuration memory in response to the security mode signal indicating a transition of the key memory from the secure mode to the non-secure mode.

16. (New) The PLD of claim 13, wherein the boundary scan control circuit is adapted to test the PLD.